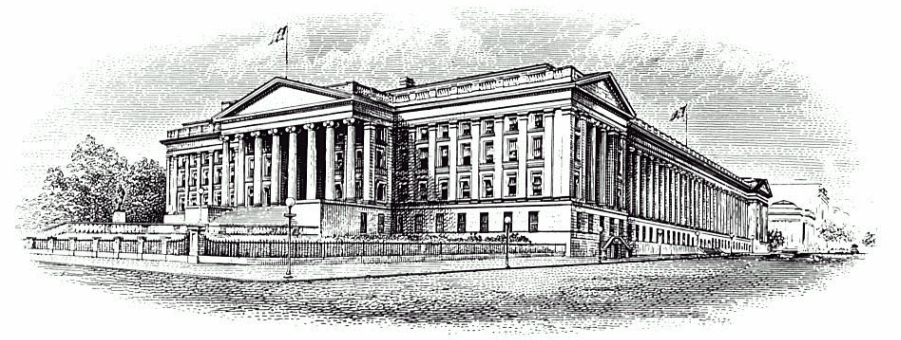

DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS

Embargoed Until 1:15 pm EST
March 19, 2003

Contact: Betsy Holahan
202-622-2960

Remarks of
Treasury Assistant Secretary for Financial Institutions Wayne A. Abernathy
To
The Exchequer Club of Washington
Washington, D.C.

The Security of Personal Financial Information

It is traditional for a speaker to begin by saying what a pleasure it is to appear before you. Usually he is lying. If truth be known, he probably approaches the podium with dread, with sweaty palms and a thumping heart. And while I cannot declare myself free of these symptoms, given what a distinguished podium this is, I confess that I have looked forward to speaking to you today with genuine pleasure.

For one reason, I see so many of my friends in this gathering. Many of you went out of your way to attend my nomination hearing, which touched me deeply and which will always be remembered by me and maybe even long remembered by my children. I did not have the opportunity to thank you then, but I do so now. Thank you for the kindness and the honor.

But I have also looked forward to speaking to you today for another reason, to discuss with you an issue of importance to every one of us and to our families, to our friends and neighbors. If you are a businessman, it is very important to your customers and of course to your business. The issue is identity theft—the fear that somewhere someone is impersonating you to engage in fraud in your name.

One of the several tasks waiting for me when I arrived at Treasury was completion of the Gramm-Leach-Bliley report on information sharing. As you know, that report was due January 1, 2002, but a lot of events intervened to cause delay, a good part of which has been Treasury's work to disrupt terrorist funding and the enactment and implementation of the Terrorism Risk Insurance Program.

Frankly, I think that we have benefited from the delay. It will be a better report because we have more experience to draw upon. But we are now in the last stages of work on the report. I hope that we will be able to publish it within a couple of weeks or so.

And so having studied the issues connected with the sharing of personal financial information—together with the views of many others who have also looked at these issues—I want to share with you today some thoughts. First, I need a context, or, as a preacher of the gospel might begin, I take as the text for my remarks today the words of Charles Dickens.

In his famous work, *A Christmas Carol*, Dickens includes the following among his opening lines:

"Old Marley was as dead as a door-nail. . . . This must be distinctly understood, or nothing wonderful can come of the story I am going to relate."

Basic Principles of Information Security

Similarly, with regard to the security of personal financial information, there are some basic principles that must be understood, or nothing wonderful can come of our efforts. And I firmly believe that wonderful things can come of our legislative efforts this year.

- First, financial services providers as well as their customers have a strong interest in protecting the security of personal financial information, that is, following prudent practices so that information is used for the benefit rather than the harm of the customer.

- Second, the sharing of information, within secure parameters reinforced by uniform national standards, has increased the access of more consumers to a wider variety of financial services, at lower costs, than ever before.

- Third, the growing problem of identity theft not only disrupts the lives of individuals and families, but it also tears at the fabric of commerce in our information age.

- Fourth, customers need to understand more easily and clearly the information-sharing practices of their financial institutions and be able to exercise a real and meaningful say in how that information is shared outside of the customer relationship.

- And, fifth, in our technology-based economy, so dependent upon accurate, timely information, uniform national standards for information sharing are as essential to fighting identity theft as they are for promoting economic growth and prosperity.

Let me expound briefly upon each of these principles.

Common Interest of Providers and Customers

- Financial services providers as well as their customers have a strong interest in protecting the

security of personal financial information, that is, following prudent practices so that information is used for the benefit rather than the harm of the customer.

For too long, there has raged one of those fruitless debates, nominally called the privacy debate, that pits the interests of businesses and their customers against one another. This debate is allowed to prosper because it is conducted under the moniker of "privacy." This vague term—privacy—allows the debate to continue because it allows people to talk past each other. Neither really knows that the other is talking about. I refuse to engage in that debate, because I am not sure what the other parties have in mind when they talk about privacy.

I think I might know what I have in mind. I have in mind what I think is better called security, security of personal financial information. By that I mean, ensuring that customers' information is used for their benefit, not for their harm. And if that is what we really mean in all of this debate, then I think that the debate can be fruitful, it can lead to specific action that will improve the security of that information. Both business and customers having a shared interest in the promotion of that security. And I see identity theft as the chief threat to that security.

Benefits to Consumers

The second basic principle: the sharing of information, within secure parameters reinforced by uniform national standards, has increased the access of more consumers to a wider variety of financial services, at lower costs, than ever before.

Here I would like to use a metaphor. All of my life I have been cursed by being an in-between size. I was always size 7—and a half, 9—and a half. Shoes, shirts, coats, never quite fit right—and my parents could never afford a tailor to give me a customized fit. Today, much has changed. Today, I can walk into a discount clothier and buy right off of the rack a suit that fits me quite well, that with a few minor adjustments can almost look tailored.

A similar thing has been happening with financial services. Back in the days when I was wearing clothes that didn't quite fit right my mother took me by the hand into the local community bank, and I opened up my passbook savings account. In those days, if you wanted a loan, you went into the bank, and the question was, do you "fit" the loan product that we have to offer? The question was yes or no, and for many, the answer was no, or "not just now, bank with us a while, open up a savings or checking account, and after we know you better we can talk."

Today, much has changed. Today, you can walk into a bank almost anywhere in the country, and 9 times out of 10, or maybe even 19 times out of 20, the answer is already "yes", you can get the loan. The application process serves to discover just what minor adjustments are necessary to price your particular risk properly. The banker may never have seen you before, never known you, but because of information sharing through the uniform standards of the Fair Credit Reporting Act, FCRA, the banker knows a million people like you and already has been able to price your risk and can offer you a product that very day that meets the needs of you and your family. Because of modern financial information sharing in America, millions of people have been brought into the financial mainstream. That is a tremendous achievement, found nowhere else on earth.

Identity Theft—Serious and Growing

The third basic principle: the growing problem of identity theft not only disrupts the lives of individuals and families, but it also tears at the fabric of commerce in our information age.

Identity theft is not a little crime. By several estimates, nearly one million people will be victimized this year, with nearly 11 million people already on the casualty list. And this is a crime that affects the whole family—as well as the firms with which they do business.

Moreover, the worst, most disruptive form of this crime is also its most virulent, where someone impersonates you and obtains his own accounts, his own credit cards, his own debts in your name, that you only find out about long after the fraud has begun, and you lose your job, your savings, your good name. By some estimates, more than 100,000 people this year will be attacked by this form of identity theft, and this strain is growing by as much as 40% per year. Experience tells me that there are several here in this room today who have been made sufferers from identity theft, or whose family members or colleagues have been victimized.

As I have discussed, many of the benefits of modern commerce rely upon the nation-wide flow of information, accurate, up-to-date, reliable information. Identity theft strikes directly at that stream and poisons it. Sure, we could stop that flow, but would it really make the information more secure? Stagnant pools of information are of no more benefit than stagnant pools of water, and are no more immune from pollution. We need to find ways to make that information stream more secure and to use it to fight identity theft. My conversations with businesses, regulators, and victims give me confidence that we can.

Easy to Understand, Easy to Exercise

The fourth basic principle: customers need to understand more easily and clearly the information-sharing practices of their financial institutions and be able to exercise a real and meaningful say in how that information is shared outside of the customer relationship.

I find few who disagree when I say that the Gramm-Leach-Bliley information-use notices have not succeeded in their goal to inform customers. The notices are not friendly to read. They are too long, too filled with jargon, designed more for lawyers than for customers. The first round of annual notices, the customers complained. The second round, the customers threw them away. The third round is not expected to be any better. Is anything disclosed if the customer does not read it? Technically, maybe, but the customer remains uninformed.

As we consider the Gramm-Leach-Bliley notices, we need to get beyond the stale discussion of opt-in or opt-out, that seldom seems to touch upon real customer needs. I think that we can do better. I have seen us do better. We have called upon industry to look at the example of nutrition labeling on food products, where we have simple, understandable, uniform disclosures that can be accessed and understood by the consumer while the consumer is making a purchase. We have asked them to craft a model for the Gramm-Leach-Bliley notices that gives the same level of real, accessible disclosure to consumers. Lately, I have seen some excellent work in this

regard.

Together with easy to understand notices, we need to provide for the easy exercise by customers of their choices under Gramm-Leach-Bliley. For the current structure of choices to work, it must be just as easy for a customer to say no to an information sharing option as it is for the customer to make a change of billing address.

Uniform National Standards

And the fifth principle: in our technology-based economy, so dependent upon accurate, timely information, uniform national standards for information sharing are as essential to fighting identity theft as they are for promoting economic growth and prosperity.

I have discussed the benefits to consumers from the FCRA's uniform national standards for information sharing, benefits of greater access to more products, at lower cost, by more people than ever before. A similar story could be told about the impact of FCRA information sharing on retailing and on economic productivity in general.

From my consultations with people involved in the fight against identity theft, I have the growing conviction of the important role that uniform national standards can play in deterring identity theft, tracking down the thieves, and restoring the records of victims. I don't know how you can make progress against identity theft without them. Anything that slows down or interrupts the flow of information by which identities can be verified or crooks tracked down creates shadows within which the identity thieves operate. And the restoration of victims' records is made harder with each new hoop or hurdle that is erected. I suspect that this awareness was part of the decision by the state banking regulators on Monday to announce their support for renewing the FCRA's uniform national standards.

Opportunity to Make a Difference This Year

There is more to this story. A lot more can be said. A lot more needs to be done. On Monday, a reporter asked me why the interest this year. Is it because the problem has become so great, or because of the expiration of the FCRA uniform standards? My answer was both. The problem is greater and growing, and we have before us what could be an ideal legislative vehicle for addressing the problem head on, a great opportunity to make a real difference in the fight against this crime this year.

And now I close with another text, this from Senate Banking Committee Chairman Richard Shelby. In a speech that he gave on December 5 of last year, he said,

"I believe we should consider privacy in the same way we do security. I have always found it somewhat interesting, that when we talk about individuals' desire to protect personal information about themselves we call it privacy and when we discuss safeguarding institutions and business information we call it security. I believe that many of the same interests are sought to be protected."

I agree. That is exactly the wonderful thing that I hope that we can do this year.